Method and Apparatus for Detecting Password Attacks Using Modeling Techniques

Abstract

5   Provided is an apparatus and method for detecting fraudulent passwords so that computer break-in attempts can be distinguished from authorized users incorrectly entering their passwords. An actual password is mapped against a computer keyboard and the resultant data is stored in memory. The profile of an entered password is compared to the stored profile. If the profile of the entered

10   password differs significantly from the stored profile, then the login attempt is flagged as an attempted intrusion. In one embodiment of the current invention, passwords are mapped according to the distance subsequent keystrokes are from each other. Different embodiments may have different mapping schemes. For example, mapping data may correspond to statistical data that corresponds to the likelihood that

15   a particular character is typed by mistake when another character is intended.